

Overview to Student Data Privacy in WI



Guidance for Department of
Public Instruction Staff and
School District Employees

This document's goal is to provide a brief overview of the aspects most relevant to Confidential Student Data Privacy in Wisconsin.

Student Data Privacy Overview

Agenda

Part 1: Data Privacy Rights & Responsibilities

Part 2: Tips for Protecting Confidential Data

Part 3: Access to Tools and/or Data

Part 4: Pertinent Laws & Policies



1. Data Privacy Rights & Responsibilities

Introduction

- In performing your official duties, you may be given access to data tools that allow you to view individual student records.
- You are legally and ethically obliged to safeguard the confidentiality of these student records.

1. Data Privacy Rights & Responsibilities

- Depending on your role, you may be able to access:
 - Student-level data
 - Summary data
 - Economic Indicators
 - Downloadable data
- **All users of the secure portal, regardless of role, are obligated to Protect Student Privacy. All secure roles enable student data access to some degree and the data is not redacted like the public portal.**

Examples of Confidential Student Data

- **Student number**
- **Attendance**
- **Habitual truancy**
- **Suspension**
- **Expulsion**
- **Dropout**
- **Course-taking**
- **Retention**
- **Test results**
- **Primary disability category**
- **Migrant status**
- **Homeless status**
- **English Language Proficiency level**
- **Educational environment**
- **Free and reduced lunch eligibility**

1. Data Privacy Rights & Responsibilities

- **The following agreement is displayed in [Secure Home](#) for all users at initial login and every 90 days thereafter.**
- **Educational data system users are required to agree to each of the statements below:**
 - I will respect and safeguard the privacy of students and the confidentiality of student data.
 - I will comply with state and federal privacy laws and all district regulations, policies, and procedures established to maintain the confidentiality of student data.
 - I will not disclose or transmit confidential data to persons not specifically authorized to access these data by the District Security Administrator, Application Administrator or District Administrator.

Agreement to Protect Student Privacy - continued

- I will use the confidential data for legitimate educational purposes only as necessary to perform my district or school assigned tasks.
- I understand that my password is as important as my signature. It is my obligation to keep my password confidential. I will not share my password with anyone.
- I will not use other users' login names or passwords.
- I have viewed the [student privacy training materials](#) and understand my obligation to protect the confidentiality of the student data that I will be accessing.

1. Data Privacy Rights & Responsibilities

Your obligations as a responsible data user include the following actions:

- Individual student data can never be publicly published or released.
- Student education data may not be released except under specific circumstances as designated by law.

Improper release of these data expose you and your district to potential criminal and civil liability, and loss of federal funds.

1. Data Privacy Rights & Responsibilities

- **Printed reports** can be shared publicly:
 - Only after you've reviewed them to ensure that no student could be identified from the report and that the data is redacted to protect the privacy of the student.
- If a reasonable person from your community could identify a student from a report, directly or indirectly, it is your responsibility to store that report in a secure place.
- Share the report only with those with a legitimate educational interest – as determined by your school board.

What data can be released?

- Summary (aggregated) data can be released but only if group size is large enough to protect the privacy of individual members of the group. Data on the [WISEdash Public Portal](#) and in District/School Report cards have been aggregated and redacted to protect privacy. The redaction method used in the District/School Report cards can be used in your district as well.
- When the identity of an individual student could be inferred due to small group size in a report, treat that report as confidential.

2. Tips for Protecting Confidential Data

When Viewing Confidential Data

Tip #1:

Make every effort to prevent unauthorized people from viewing your screen while you are accessing confidential information.

Tip #2:

When you are finished with the data tools, log off and close any windows containing data or reports.

Tip #3:

Avoid writing down Login/Password information in a location viewable by potentially unauthorized people.

2. Tips for Protecting Confidential Data

On Electronic Devices

Tip #1:

Always store Sensitive PII on a shared **secure** drive rather than your computer hard drive or shared unsecured drive.

Tip #2:

Lock your computer screen when away from your computer by pressing “CTRL + ALT + DEL” then “Lock this Computer”.

Tip #3:

Do not have your computer remember passwords (Chrome, Internet Explorer, etc.)

3. Access to Tools and/or Data

Access to Public Tools

WISEdash is used by districts, schools, parents, researchers, media, and other community members to view data published by DPI.

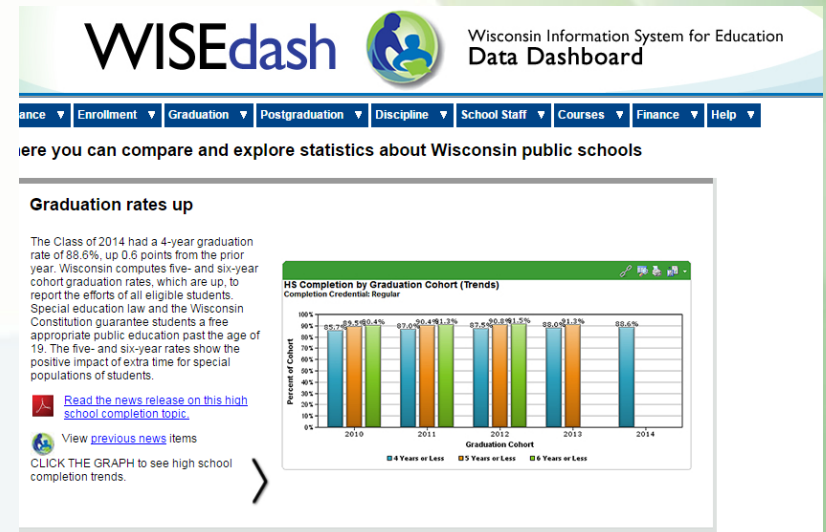
PII data on the portal are summarized and redacted to protect student privacy.



3. Access to Tools and/or Data

Public Tools

Current and certified data can be displayed for multiple years and it can be grouped and filtered by a variety of demographics including grade level, gender, race/ethnicity, economic status, disability, English proficiency, and migrant status. Data download files are also available.



3. Access to Tools and/or Data

Access to Secure Tools

Access to secure DPI tools is available through Secure Home once access has been granted by a security administrator.

Secure Home is a secure webpage used by authorized individuals to access DPI's secure applications and tools in one location.

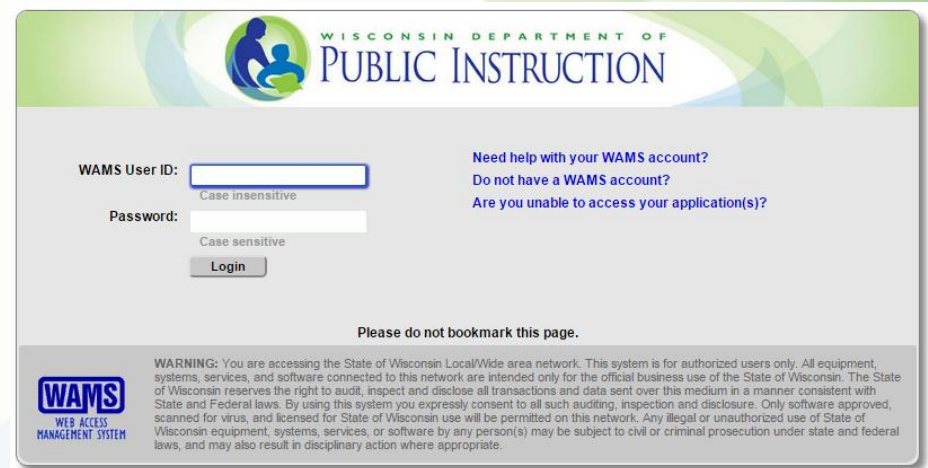


3. Access to Tools and/or Data

You will need:

A personal WAMS ID

Your District Security Administrator / WISEdash Application Administrator to grant you access to a Secure Home Application



The screenshot shows the WAMS login interface. At the top, the Wisconsin Department of Public Instruction logo is displayed. Below the logo, there are two input fields: 'WAMS User ID:' and 'Password:'. The 'WAMS User ID' field has a placeholder text 'Case insensitive'. The 'Password' field has a placeholder text 'Case sensitive'. A 'Login' button is located below the password field. To the right of the login fields, there are three links: 'Need help with your WAMS account?', 'Do not have a WAMS account?', and 'Are you unable to access your application(s)?'. Below the login fields, there is a warning message: 'Please do not bookmark this page.' At the bottom left, there is a logo for 'WAMS WEB ACCESS MANAGEMENT SYSTEM'. At the bottom right, there is a detailed warning text: 'WARNING: You are accessing the State of Wisconsin LocalWide area network. This system is for authorized users only. All equipment, systems, services, and software connected to this network are intended only for the official business use of the State of Wisconsin. The State of Wisconsin reserves the right to audit, inspect and disclose all transactions and data sent over this medium in a manner consistent with State and Federal laws. By using this system you expressly consent to all such auditing, inspection and disclosure. Only software approved, scanned for virus, and licensed for State of Wisconsin use will be permitted on this network. Any illegal or unauthorized use of State of Wisconsin equipment, systems, services, or software by any person(s) may be subject to civil or criminal prosecution under state and federal laws, and may also result in disciplinary action where appropriate.'

Data Requests

Any non-DPI personnel requests for Confidential Data are referred to the **DPI Data Request Process**

Webpage:
http://wise.dpi.wi.gov/wise_datarequests

Wisconsin DPI Data Request Process

The Wisconsin Department of Public Instruction (DPI) collects and maintains data about education in the State of Wisconsin required for State and Federal reporting including data such as student data, school finance data, teacher licensing data, school performance data, and agency data. Individuals can request data through the process described below.

New Data Requests

[Public Data Request Information](#)

[Confidential Data Request Information](#)

Existing Confidential Requests:

[Request Changes to an Existing Confidential Data Use Agreement \(DUA\)](#)

4. Pertinent Laws and Policies

- What laws guide us in the protection and the responsible use of educational data and student privacy?

4. Pertinent Laws and Policies

Confidential Data Privacy is governed at two levels:

State - (Wisconsin Pupil Records Law)

Federal - (FERPA)

4. Pertinent Laws and Policies

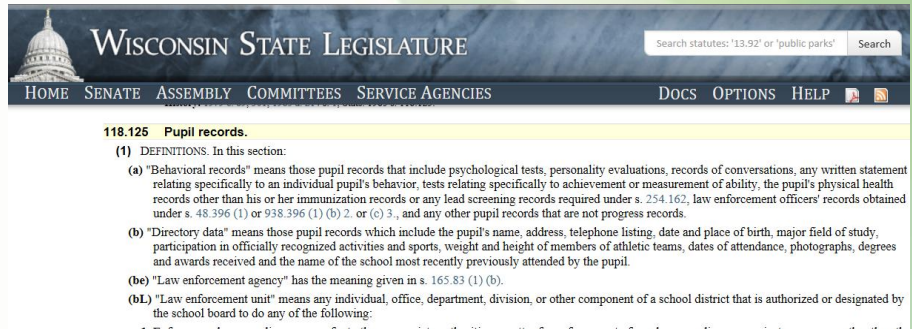
Wisconsin Pupil Records Law:

Wisconsin state law regarding the protection and privacy of students records.

Family Educational Rights and Privacy Act (FERPA):

Federal law providing parents certain rights regarding their children's educational records

Important: Violations of FERPA can jeopardize a district's federal funds.



Directory Data as Quoted in WI Pupil Records Law

[Wisconsin Pupil Records Law 118.125](#), 1973 (click the link for the full text)

(b) “ Directory Data means those pupil records which include the pupil's name, address, telephone listing, date and place of birth, major field of study, participation in officially recognized activities and sports, weight and height of members of athletic teams, dates of attendance, photographs, degrees and awards received and the name of the school most recently previously attended by the pupil.”

DPI Guidance Regarding Directory Information

School districts have the authority to limit what will be treated as directory information. That is, a school district may choose to designate some, but not all of the information defined in state and federal law, as directory information. For instance, some Wisconsin school districts do not designate a student's address or phone number as directory information for privacy reasons.

[FERPA](#), 1974 (click the link for the full text)

[Guidance for Parents](#)

Schools must notify parents and eligible students annually of their rights under FERPA. The actual means of notification (e.g., special letter, inclusion in a PTA bulletin, student handbook, newspaper article, etc.) is left to the discretion of each school district. Parents must be allowed at least 14 days to notify the school district that directory information may not be shared without their consent.

Additional Applicable Laws Related to Data and Privacy

Federal

COPPA - [Children's Online Privacy Protection Act](#)

IDEA - [Individuals with Disabilities Act](#)

NSLA - [National School Lunch Act](#)

PPRA - [Protection of Pupil Rights Amendment](#)

Wisconsin

Wisconsin Statute 115.297 - [Cooperative Research on Education Programs; State Student Data System](#)

Wisconsin Statute 118.19 [Teacher Certification and Licenses](#)

Conclusion

For additional information, please reference DPI's [Data Privacy](http://wise.dpi.wi.gov/wise_studentdataprivacy) page at: http://wise.dpi.wi.gov/wise_studentdataprivacy

Student Data Privacy Main Menu

